

Fig. 1a

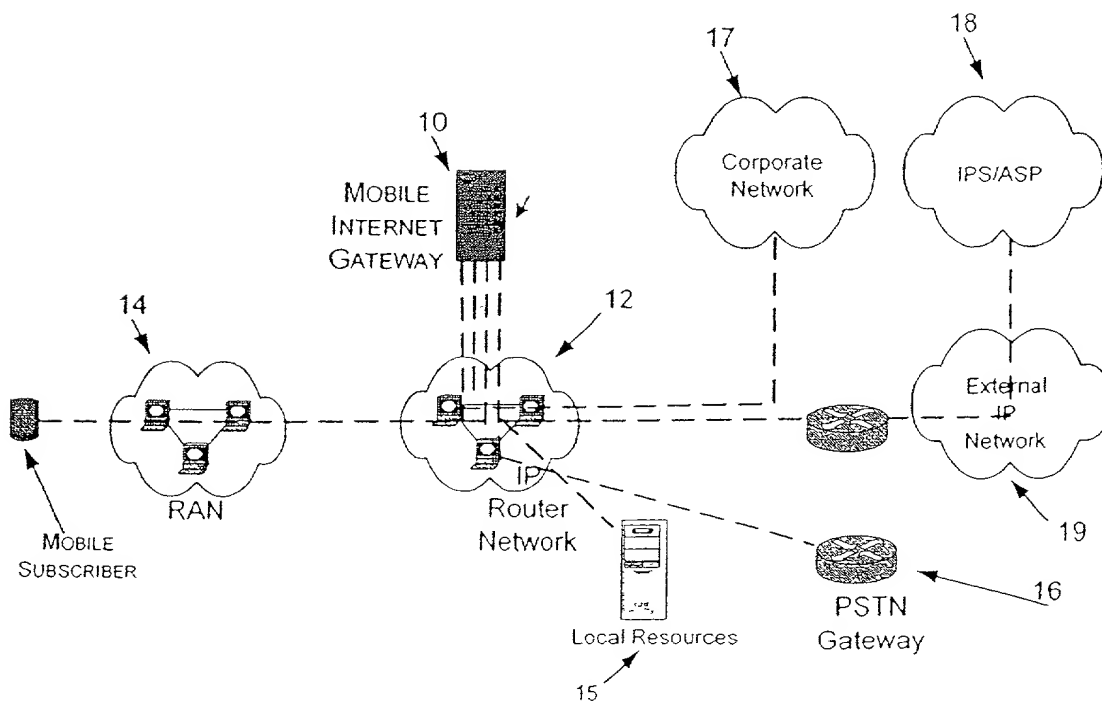


Fig. 1b

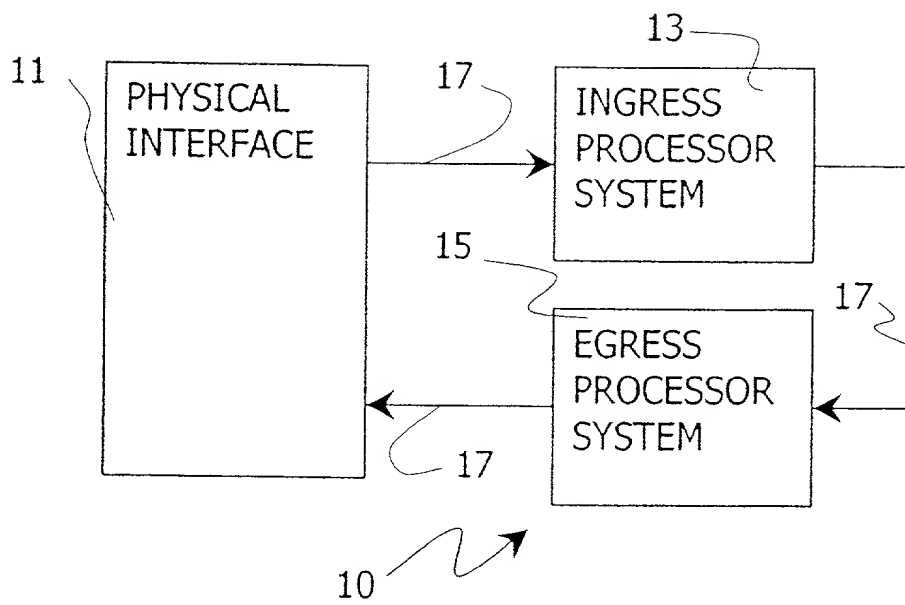


Fig. 2A

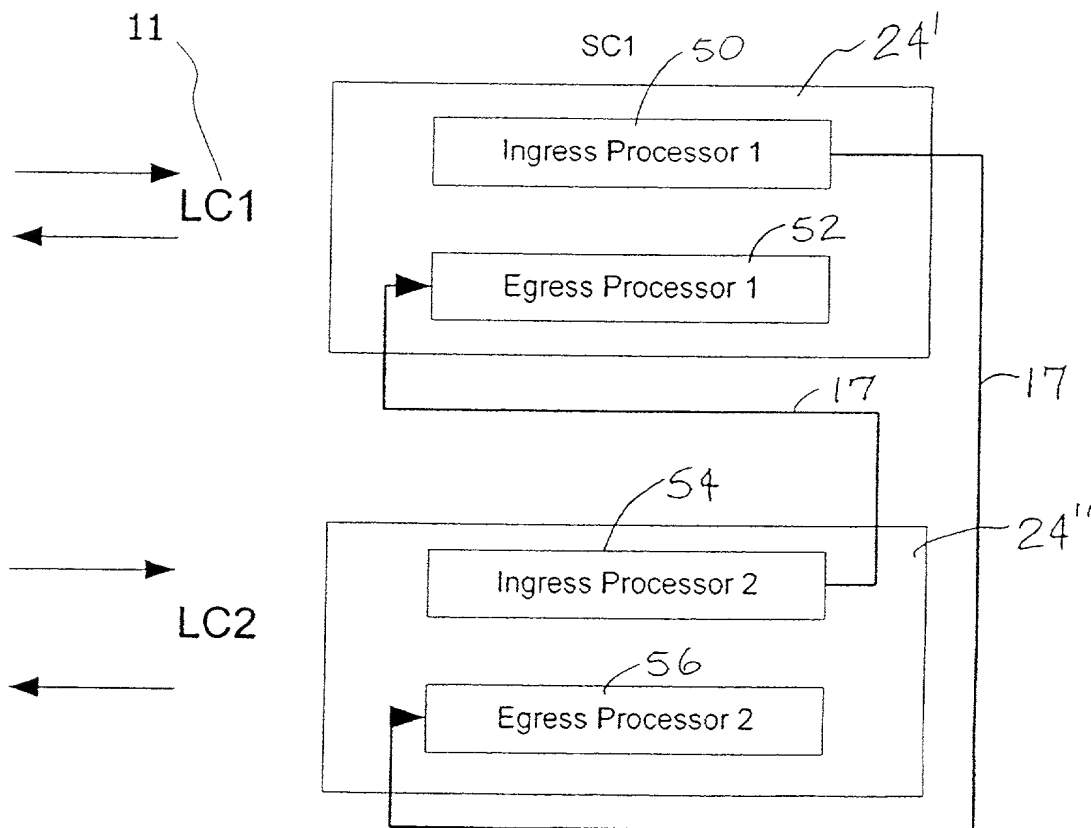


Fig. 2B

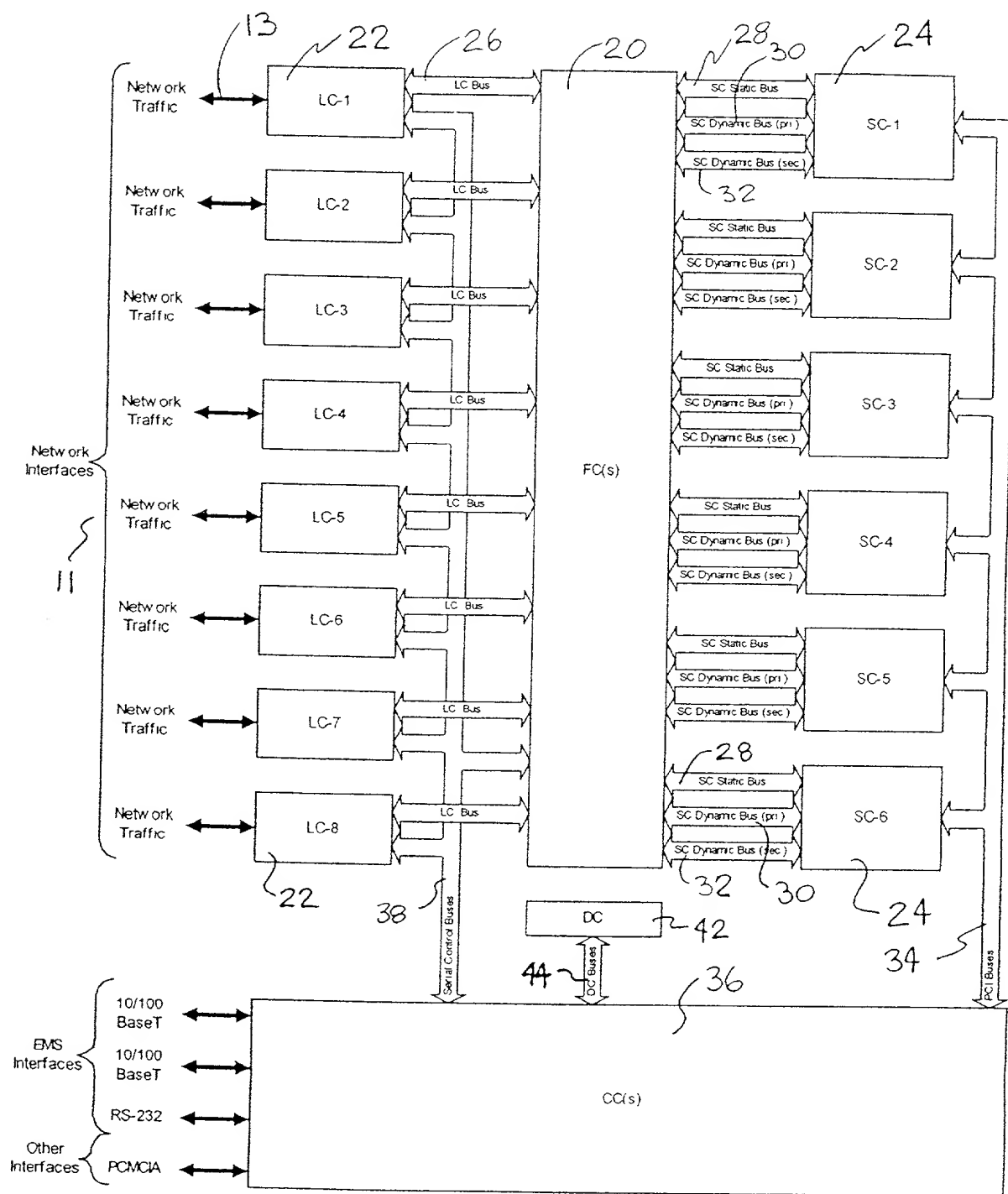


Fig. 3

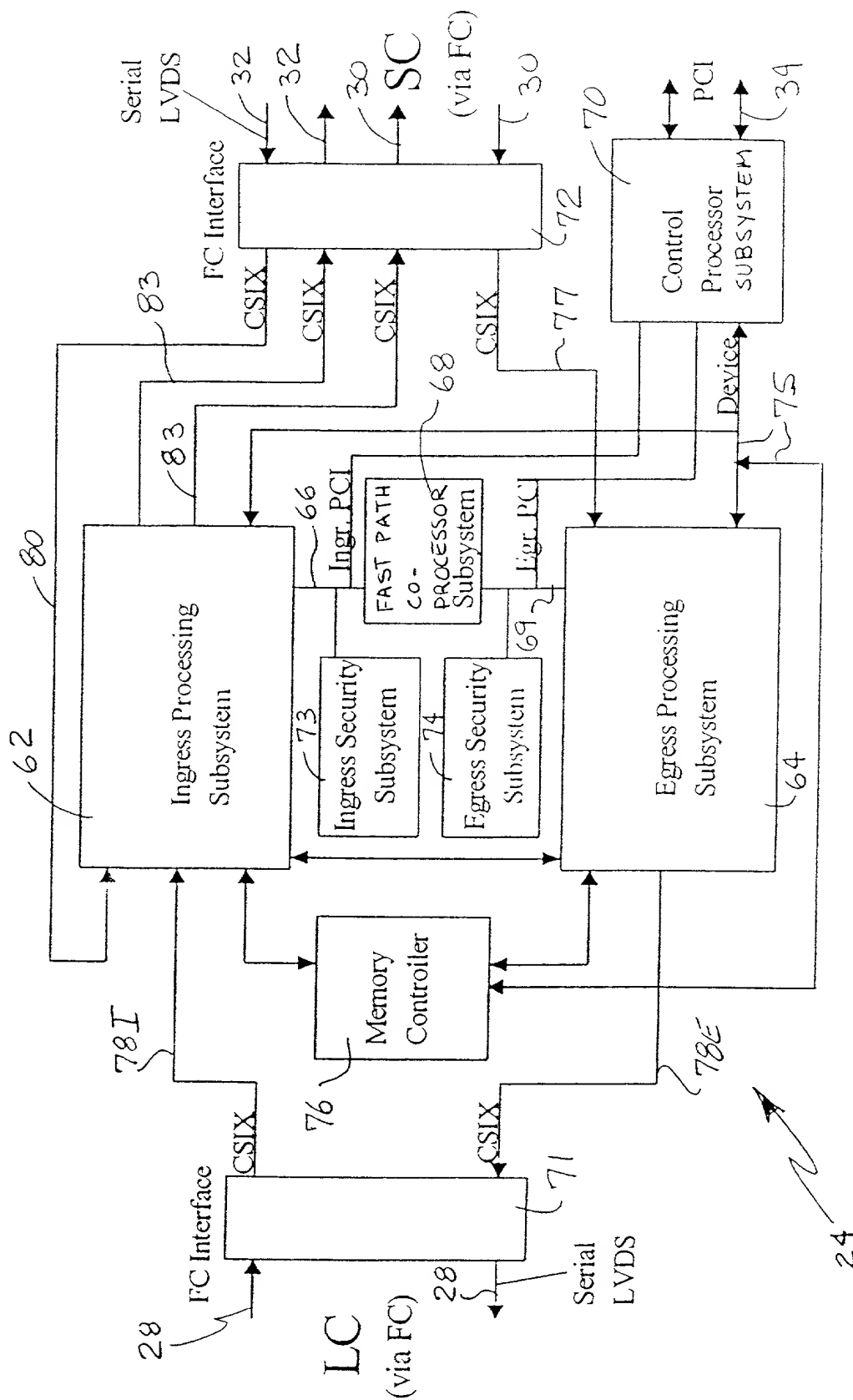


Fig. 4

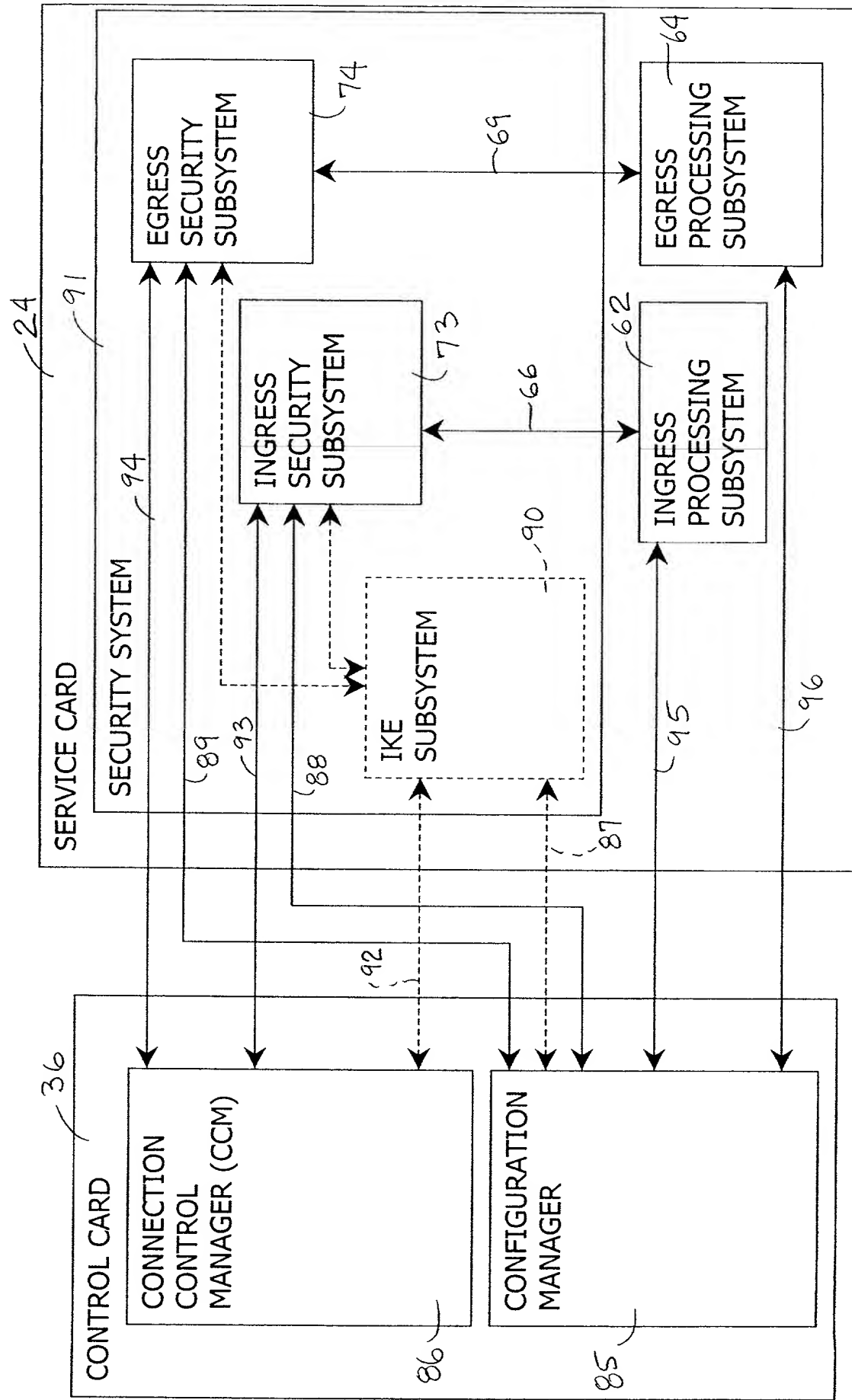


Fig. 5

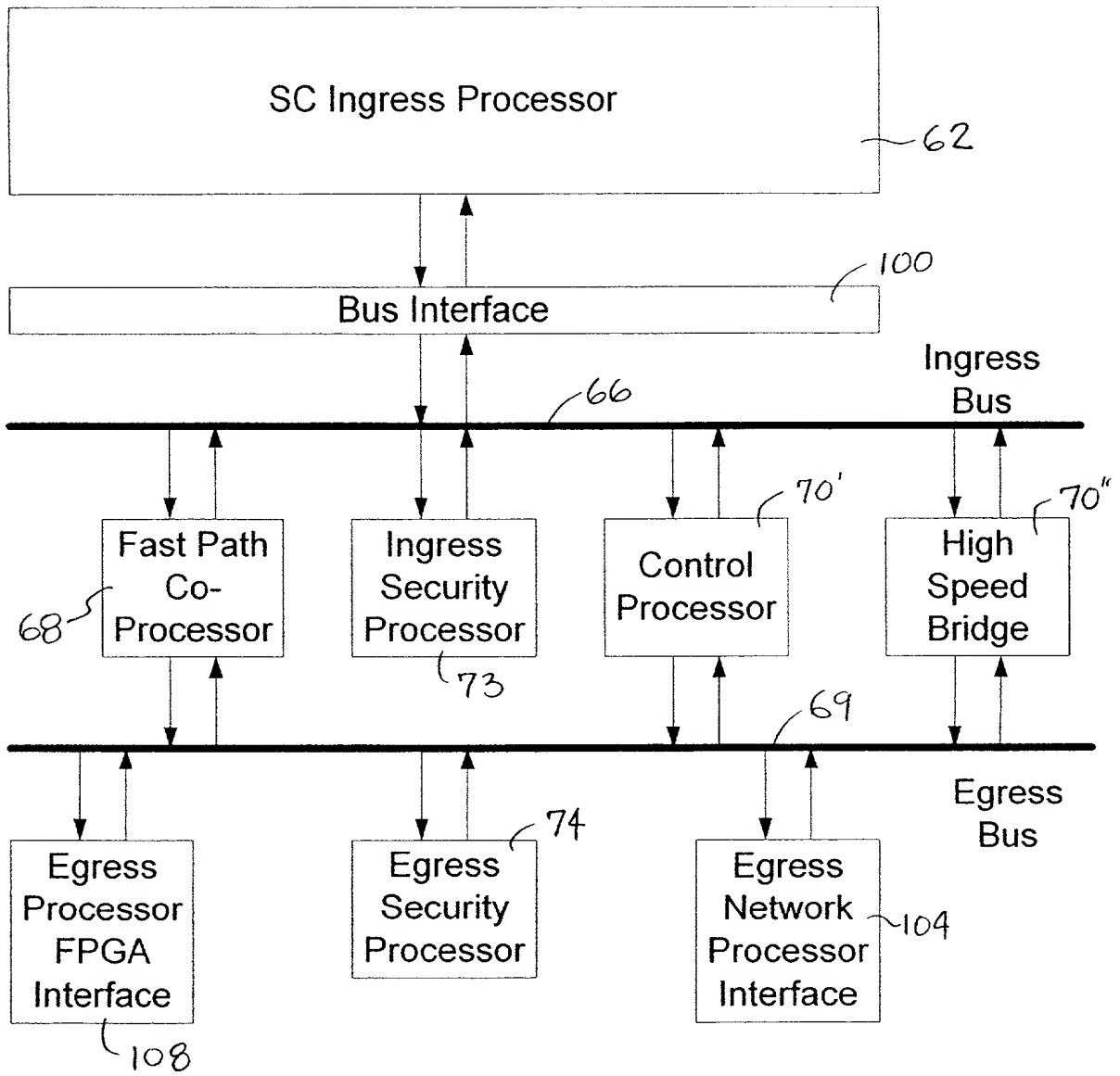


Fig. 6

700
THE TWO SECURITY ASSOCIATIONS, AT THE SECURITY SUBSYSTEMS, ESTABLISH A SHARED SECRET KEY TO BE USED FOR SYMMETRIC BLOCK ENCRYPTION (E.G., A DIFFIE-HELLMAN KEY EXCHANGE).

702
USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION

704
MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER

706
A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD

708
THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM

710
KEY, ENCRYPT SESSION DATA

712
FORM AND SEND SECURITY MESSAGE INCLUDING AUTHENTICATION FOR AUTHENTICATING THE TRANSMISSION OF THE SESSION DATA

714
CHECK AUTHENTICATION AT RECEIVER SUBSYSTEM

716
DECRYPT THE SM BY THE RECIPIENT USING THE SHARED SECRET KEY OF STEP 700. THE DECRYPTED SESSION DATA IS THEN LOADED INTO THE SECURITY SUBSYSTEM TABLES.

Fig. 7A

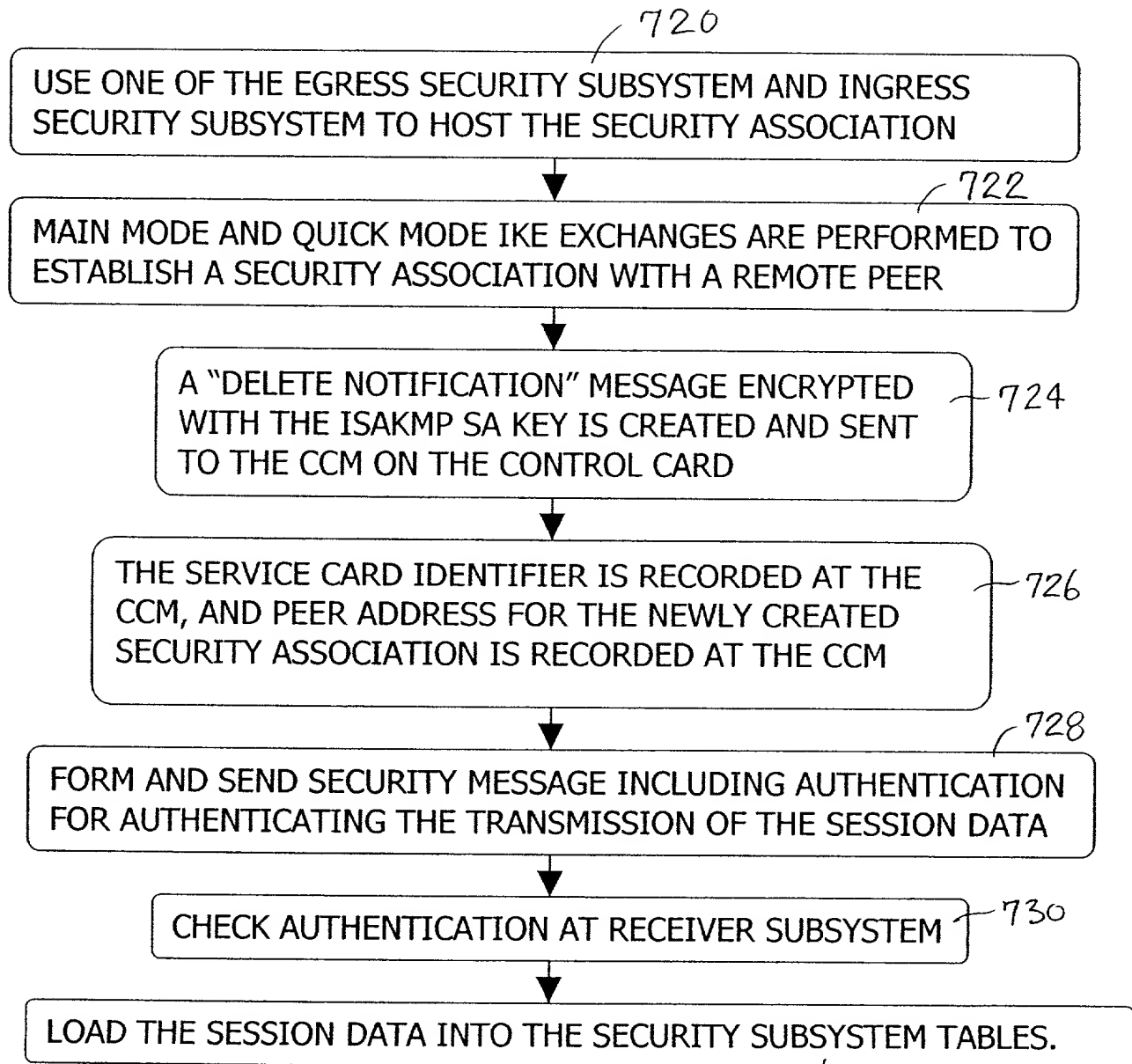


Fig. 7B

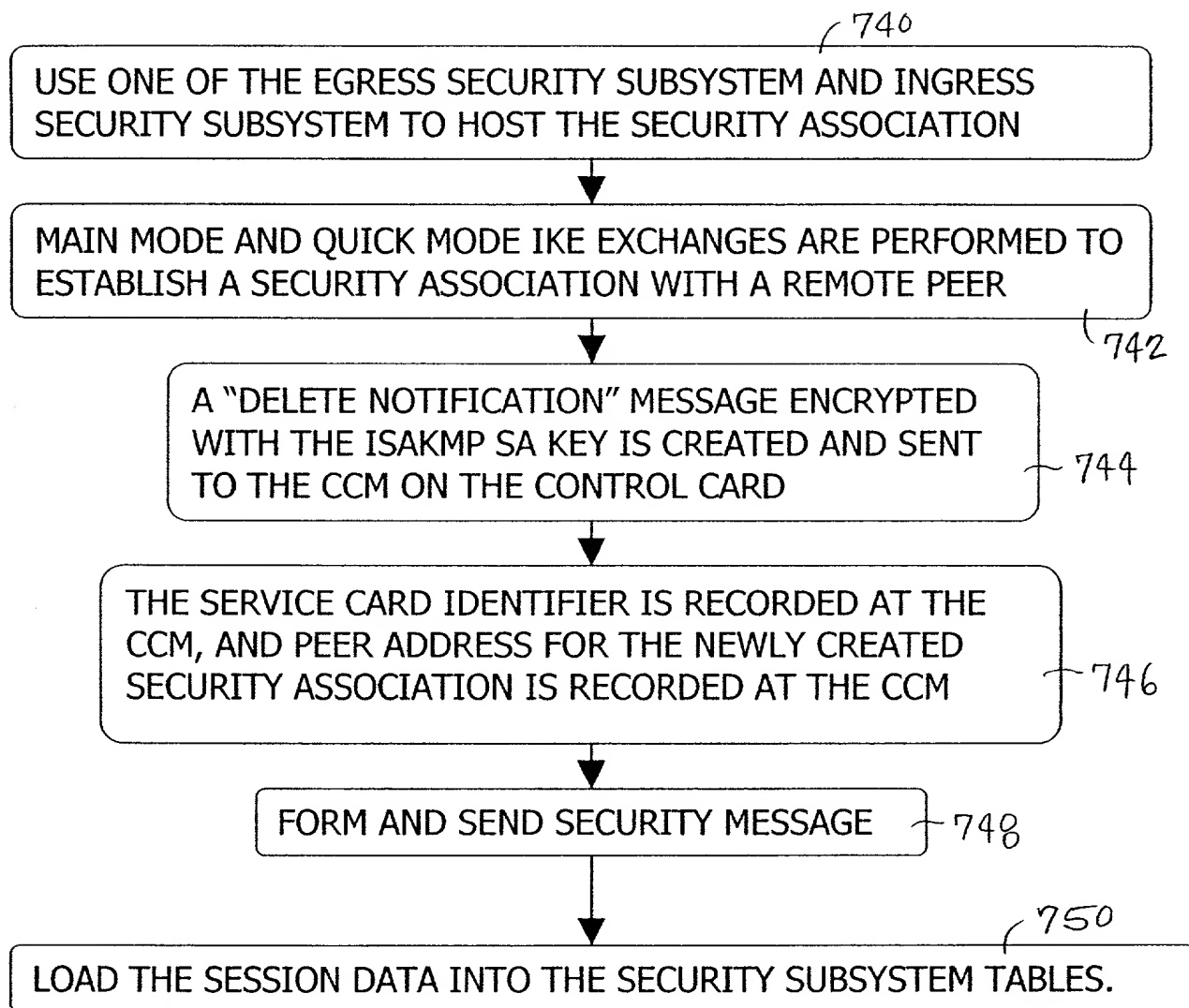


Fig. 7C

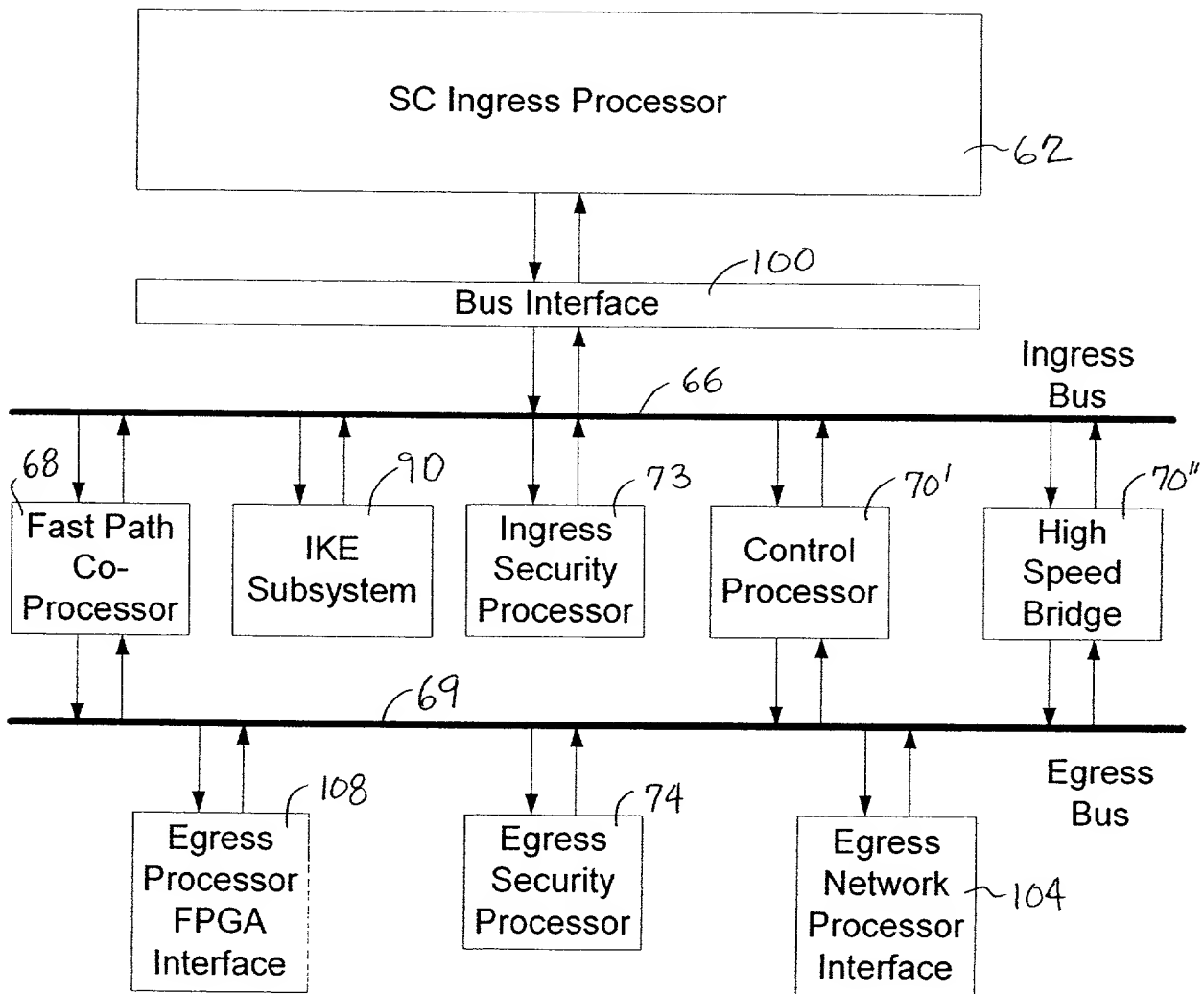


Fig. 8